UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/629,408	08/01/2000	Francis M. Anton Jr.	35817/0269827	6059

24943 7590 03/01/2004

INTELLECTUAL PROPERTY LAW GROUP LLP
12 SOUTH FIRST STREET
SUITE 1205
SAN JOSE, CA 95113

EXAMINER	
QUINONES, EDEL H	
ART UNIT	**PAPER NUMBER**
2131	8

DATE MAILED: 03/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/629,408	ANTON JR. ET AL.	
	Examiner	Art Unit	
	Edel H Quinones	2131	

-- The MAILING DATE of this c mmunication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

III. Detailed Action

1. Claims 1-32 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed on 11/14/02 complies with the provisions of MPEP § 609. It has been placed in the application file, and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 12 recites the limitation "said hidden reserved field and authentication information from said solicited data packet" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

4. Claim16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 16 recites the limitation "said second identification keyword" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim1-2 and 12-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Short et al. (U.S. Patent 6,636,894 and Short hereinafter)

In regards to claim 1, Short teaches a system for controlling Internet access on a network (i.e. a universal network gateway) (col. 1, lines 15-16), said system comprising:

at least one access device for connecting to said network and for originating out-going data packets (i.e. computer) (figure 1, #14), each of said at least one access device being characterized by a unique hardware address (i.e. MAC address) (col. 8, lines 8-15);

a redirection server (i.e. the functionality of the redirection server is integrated into the network itself) (col. 8, lines 20-23) accessible via the Internet;

a network monitoring device for monitoring out-going data packets sent from said network to the Internet and for verifying if an originator access device of an out-going data packet is authorized for Internet access (i.e. gateway device) (col. 8, lines 31-42),

all out-going packets originated from authorized access devices being forwarded unimpeded to the Internet (i.e. the AAA server will create a user profile utilizing this information

so that the user will be able to obtain immediate access to the network next time the user logs in without being required to enter login information again.) (col. 13, lines 22-26)

and all outgoing data packets originated from unauthorized access devices be being inspected for determination of their target destination Internet websites, and for checking if a determined target destination Internet website matches a predetermined authentication server website and forwarding a corresponding out-going data packet to said predetermined authentication server if a match is found,

said network monitoring device responding to a match not being found by disregarding the determined destination Internet website and forwarding the out-going data packet to said redirection server (i.e. where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page. The login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device) (col. 13, lines 7-12);

whereby all out-going data packets to the Internet gain access to the Internet irrespective of whether their respective originator access devices are authorized for Internet access (i.e. the login page can be an external webserver) (col. 12, lines 61-63).

In regards to claim 2, Short teaches that said redirection server responds to a received data packet from an unauthorized originator access device by sending said originator access device a message instructing it to connect to said predetermined authentication server (i.e. the originator device is redirected to a login page) (col. 8, lines 65-67).

In regards to claim 12, Short teaches that the authentication server responds to a solicited data packet having a hidden field by extracting the contents of the hidden reserved field and authentication information, and sending the extracted information to a gate keeper server (i.e. after receiving a request for access from a user, and identifying the user or location, the AAA server determines the access rights of the particular user.) (col. 12, lines 21-24). It can be inferred that the user and location are identified by extracting the contents of the hidden fields (i.e. account ID, hardware address, session ID, etc.)

In regards to claim 13, Short teaches that the gate keeper server (i.e. AAA server) is accessible via the Internet. That is, Short teaches that the AAA server can be located within the gateway device (col. 4, lines 54-55), and that the gateway device is connected to the Internet (col. 2, lines 13-18)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3-5 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Mishkin (U.S. Patent 6,377,781)

In regards to claim 3, Short teaches that said authentication server responds to an unsolicited received data packet by sending an originator access device of said data packet a questionnaire form (i.e. login page) soliciting authentication information (i.e. user's name, address, credit card number etc.) (col. 8, lines 65-67).

Short does not teach that the questionnaire form includes a hidden reserved field and a first identification keyword.

Mishkin discloses a system for implementing and manipulating a session for a computer-based quiz (col.1, lines 10-11). Mishkin teaches that the questionnaire form includes a hidden reserved field and a first identification keyword (i.e. at the top of the page are three fields: "instructor ID", "session name", and "student name". There is also a hidden field quizID pre-populated with "1234".) (col. 8, lines 1-3).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Short with the teachings of Mishkin to include a questionnaire form that included a hidden reserved field and a first identification keyword with the motivation to facilitate administration of the questionnaire forms (Mishkin, col. 1, lines 45-46).

In regards to claim 4, Mishkin teaches that said hidden reserved field is not accessible by said originator access device which receives said questionnaire form. Mishkin teaches that the hidden field is pre-populated with "1234". This and the fact that the field is hidden suggest that the field cannot be accessed by said originator access device.

In regards to claim 5, the combination of Short and Mishkin teaches the system of claim 3 as discussed above.

The combination of Short and Mishkin does not teach that the first identification keyword is based on address information from the network monitoring device.

The Examiner takes Official Notice that it is old and well established in the art the fact that an identification keyword can be based on address information such as an IP address (see Short col. 7, lines 10-24). This provides an easy and efficient way of identifying the source and destination of data packets in a network.

Therefore, it would have been obvious to one of ordinary skill in the art to use a first identification keyword based on address information form the network monitoring device because to modify the combination of Short and Mishkin to include that the first identification keyword is based on address information, such as an IP address, from the network monitoring device in order to facilitate the identification of information source.

In regards to claim 11, Short teaches that the originator access device receiving the questionnaire form uses web browsing software to supply the solicited authentication information into the questionnaire form before transmitting the questionnaire form back to the authentication server via the Internet (i.e. the users can be directed to a webserver [external or internal] where the users have to login and identify themselves) (col. 12, lines 61-63).

8. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Mishkin as applied to claim 3, in further view of Levy (U.S. Patent 6,4,66,981)

In regards to claim 6, the combination of Short and Mishkin teaches the system of claim 3 as discussed above.

The combination of Short and Mishkin does not teach that before forwarding data to the authentication server, the network monitoring device scans contents the data packet in search of the first identification keyword and upon locating said first identification keyword, it generates a second identification keyword based on the unique hardware address of the originator access device, the second identification keyword being inserted in the hidden reserved field.

Levy teaches a system for connecting a computer to a communication system (col. 1, lines 6-7). Levy teaches the generation and transmission of an identification keyword based on the unique hardware address of the originator access device when a device connects to an authentication server (col. 9, lines 25-41).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Short and Mishkin with the teachings of Levy to include the generation and addition of a second identification keyword based on the hardware address of the originating device with the motivation to provide an efficient technology that avoids loading a large software program onto the computer (col. 2, lines 25-26).

The combination of Short, Mishkin and Levy however does not teach that the second identification keyword is inserted in the hidden reserved fields.

Guthrie teaches a personal authentication system. Guthrie teaches that an API reduces some of the processing overhead required for user authentication by the server 104. When the user is, for example, entering data to a form on a web page to request a certain process to be

performed (e.g., by a common gateway interface (CGI) program), the user's account ID and previously generated response are attached to the form as a hidden field (col. 14, lines 28-48).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Mishkin and Levy with the teaches of Guthrie to include that the second identification keyword is inserted in the hidden reserved fields with the motivation to reduce the overhead required for user authentication.

In regards to claims 7 and 8, Short teaches that a user can be identified by different means such as the user's location (col. 8, line 9) or session information such as the IP address assigned to an individual computer when the computer logs onto the network (col. 7, lines 18-21). Therefore it would have been obvious to one of ordinary skill in the art to use any of the above in addition to a hardware address to identify a user because they are all art recognized ways of identifying a user.

9. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Mishkin in view of Levy as applied to claim 6 above, in further view of Lin (U.S. Patent 6,285,683).

In regards to claim 9, the combination of Short, Mishkin and Levy teaches the system of claim 6 as discussed above. It, however, does not teach that the hidden reserved field is located within the out-going data packet a predetermined number of bytes away from said first identification keyword.

Lin discloses an invention that relates to data communications and telecommunications, and more particularly to automated services that may be provided to telephone and computer users via a telephone network (col. 1, lines 7-10). Lin teaches that the hidden reserved field is located within the out-going data packet a predetermined number of bytes away from the first identification keyword (col. 10, tables 1 and 2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Mishkin and Levy with the teachings of Lin to include that the hidden reserved field is located within the out-going data packet a predetermined number of bytes away from said first identification keyword with the motivation to maintain or utilize state information (see Lin, col. 9, lines 29-52).

In regards to claim 10, the combination of Short, Mishkin and Levy teaches the system of claim 6 as discussed above. It, however, does not teach that the hidden reserved field is immediately preceded by the first identification keyword within the out-going data packet.

Lin teaches that when the server logic means returns a data packet, the channel ID and new state value are then hidden in the next HTML page that is sent to the web browser 211. In other words, each web page is used as a storage medium for maintaining channel ID and state values for each ongoing session with a user of the web browser 211 (col. 10, lines 1-7). In other words, the Channel ID precedes the hidden reserved field (i.e. state value).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Mishkin and Levy with the teachings of Lin to include that the hidden reserved field is immediately preceded by the first identification keyword

within the out-going data packet with the motivation to maintain or utilize state information (see Lin, col. 9, lines 29-52).

10. Claims 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Reiche (U.S. Patent 6,092,196)

In regards to claim 14, Short teaches the system of claim 1 as discussed above.

Short does not teach that the authentication server uses a CGI script to parse the extracted information from the solicited data packet.

Reiche discloses a system relating to the field of computer network security (col. 1, lines 5-6). Reiche teaches that Common Gateway Interface (CGI) is a standard for interfacing external applications with information servers, such as HTTP or Web servers (col. 2, lines 37-58).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Short with the teachings of Reiche to use a CGI script to parse the extracted information form the solicited data packet with the motivation of leveraging the benefits provided by a standard for interfacing external applications with information servers, such as HTTP or Web servers.

11. Claims 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Sitaraman et al. (U.S. Patent 6,212,561 and Sitaraman hereinafter)

In regards to claim 15, Short teaches that the gate keeper server (i.e. AAA server) compares said authentication information with a predefined database to determine if the

originator access device is registered (i.e. a user profile database stores whether users have valid access rights) (col. 12, lines 21-55) (i.e. the next time the user attempts to login the user's profile will be located in the user profile database, the user's access right determined, and the user allowed transparent access to networks or services (col. 13, lines 31-33).

Short does not teach that the gate keeper responds to the verification of the originator access device being registered by sending an unblock message to said network monitoring device.

Sitaraman discloses a system for securing user domain access in a computer network (col. 1, lines 7-8). Sitaraman teaches that the gate keeper responds to the verification of the originator access device being registered by sending an unblock message to said network monitoring device (i.e. when the AAA server receives an access-request packet from an authorized SSG client, it consults the data bank of service profiles and makes a match based on the user information provided in the request. In order to access the individual profile a match must be made between the password entered by the user and the password tied to the service profile. If the passwords match, and all other requirements are met, then at step 62, the AAA server sends the SSG an "access-accept" packet in response.) (col. 6, lines 43-51).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Short with the teachings of Sitaraman to include that the gate keeper responds to the verification of the originator access device being registered by sending an unblock message to said network monitoring device with the motivation of providing adequate security precautions (see Sitaraman, col. 4, lines 31-32).

In regards to claim 18, Short does teach not that the network monitoring device responds to receipt of the unblock message by updating a network access list to authorize the originator access device for Internet access.

Sitaraman teaches that after receipt of the unblock message (i.e. the "access-accept" packet), the gateway device assesses the data within the service profile to determine whether or not a sequential only attribute exists within the service profile for the particular private domain site which the user has requested access to (col. 6, lines 51-58).

A network access list is a type of service profile for a particular private domain site. Therefore Sitaraman teaches the accessing a network access list upon receipt of an unblock message. Given that an "update" is a type of "access" to data, it can be inferred that Sitaraman teaches updating a network access list upon receipt of an unblock message.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the combination of Short and Sitaraman to include that the network monitoring device responds to receipt of the unblock message by updating a network access list to authorize the originator access device for Internet access, as taught by Sitaraman, with the motivation of securing user domain access in a computer network (see Sitaraman, col. 1, lines 7-8).

12. Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Sitaraman in further view of Levy.

In regards to claim 16, the combination of Short and Sitaraman teaches the system of claim 15 as discussed above.

The combination of Short and Sitaraman does not teach that the unblock message is encrypted with the second identification keyword.

Levy teaches that the second identification keyword could consist of an encryption key (i.e. The response message includes the MAC address of the computer 410 and an optional encryption key for communications with the computer 410.) (col. 9, lines 33-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short and Sitaraman with the teachings of Levy to include that the unblock message is encrypted with the second identification keyword with the motivation of increasing the security of data communications.

In regards to claim 17, Levy teaches that upon verification of the originator access device (i.e. access software application 411 in the portable computer 410) being registered, the gate keeper server decodes the contents of the hidden reserved field to determine the unique hardware address of the originator access device (i.e. MAC address) and that it labels the unblock message with said hardware address.

That is, Levy teaches that communication with the access software application is conducted by using a MAC address (col. 10, lines 21-36). Given that sending an unblock message is a way of communicating with the originator device, one can infer that a MAC address could be attached to the message, or that the message could be labeled with a MAC address. One would be motivated to label the unblock message with the MAC address of the originator device given the suggestion in Levy that this is a method of correctly representing the user (see Levy, col. 9, lines 65).

13. Claims 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Levy in view of Guthrie in further view of Sitaraman.

In regards to claim 19, Short teaches a system for remotely authenticating a user on a private network via the Internet (i.e. a system including an Authentication, Authorization and Accounting server) (see Abstract), the system comprising:

a network access device (i.e. computer) (figure 1, #14) for permitting said user access to said private network, said access device being characterized by a unique hardware (i.e. MAC address) (col. 8, lines 8-15);

an authentication server (i.e. AAA server) (col. 4, lines 42-50) accessible via the Internet;

a network monitoring device for monitoring the destination address of all out-going messages from said private network to the Internet (i.e. where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page. The login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device) (col. 13, lines 7-12)

Short does not teach that the monitoring device scans the content of any message whose destination is the authentication server to search for a first predetermined identification code in said message, that the network monitoring device responds to the detection of the first predetermined identification code by generating a second identification code based on the hardware address of the access device that originated the message, and by inserting the second identification code in the message before forwarding the message to said authentication server;

Levy teaches a system for connecting a computer to a communication system (col. 1, lines 6-7). Levy teaches the generation and transmission of an identification keyword based on the unique hardware address of the originator access device when a device connects to an authentication server (col. 9, lines 25-41).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Short with the teachings of Levy to include that the monitoring device generates a second identification code based on the hardware address of the access device that originated the message, with the motivation to provide an efficient technology that avoids loading a large software program onto the computer (col. 2, lines 25-26).

Guthrie teaches a personal authentication system. Guthrie teaches that an API reduces some of the processing overhead required for user authentication by the server 104. When the user is, for example, entering data to a form on a web page to request a certain process to be performed (e.g., by a common gateway interface (CGI) program), the user's account ID and previously generated response are attached to the form as a hidden field (col. 14, lines 28-48).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short and Levy with the teaches of Guthrie to include that the second identification keyword is inserted in the hidden reserved fields with the motivation to reduce the overhead required for user authentication.

The combination of Short, Levy and Guthrie does not teach that the authentication server responds to receipt of the forwarded message from the network monitoring device by decoding the hardware address the said second identification code; then generating a third identification

code based on the hardware address and by transmitting such identification code along with an unblock message to the network monitoring device.

Sitaraman discloses a system for securing user domain access in a computer network (col. 1, lines 7-8). Sitaraman teaches that the gate keeper responds to the verification of the originator access device being registered by sending an unblock message to said network monitoring device (i.e. when the AAA server receives an access-request packet from an authorized SSG client, it consults the data bank of service profiles and makes a match based on the user information provided in the request. In order to access the individual profile a match must be made between the password entered by the user and the password tied to the service profile. If the passwords match, and all other requirements are met, then at step 62, the AAA server sends the SSG an "access-accept" packet in response.) (col. 6, lines 43-51).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Short, Levy and Guthrie with the teachings of Sitaraman to include that that the authentication server responds to receipt of the forwarded message from the network monitoring device by transmitting an unblock message to the network monitoring device with the motivation of providing adequate security precautions (see Sitaraman, col. 4, lines 31-32).

Levy also teaches that upon verification of the originator access device (i.e. access software application 411 in the portable computer 410) being registered, the gate keeper server decodes the contents of the hidden reserved field to determine the unique hardware address of the originator access device (i.e. MAC address) and that it labels the unblock message with said hardware address.

That is, Levy teaches that communication with the access software application is conducted by using a MAC address (col. 10, lines 21-36). Given that sending an unblock message is a way of communicating with the originator device, one can infer that a MAC address could be attached to the message, or that the message could be labeled with a MAC address. One would be motivated to label the unblock message with the MAC address of the originator device given the suggestion in Levy that this is a method of correctly representing the user (see Levy, col. 9, lines 65).

In regards to claim 20, the combination of Short, Levy, Guthrie and Sitaraman teaches the method of claim 19 as discussed above.

The combination of Short, Levy, Guthrie and Sitaraman does not teach that the network monitoring device responds to the unblock message by updating a network access list to authorize for Internet access the user whose network access device has the same hardware address as is embedded in the third identification code.

Sitaraman further teaches that after receipt of the unblock message (i.e. the "access-accept" packet), the gateway device assesses the data within the service profile to determine whether or not a sequential only attribute exists within the service profile for the particular private domain site which the user has requested access to (col. 6, lines 51-58).

A network access list is a type of service profile for a particular private domain site. Therefore Sitaraman teaches the accessing of a network access list upon receipt of an unblock message. Given that an "update" is a type of "access" to data, it can be inferred that Sitaraman teaches or suggests updating a network access list upon receipt of an unblock message.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the combination of Short, Levy, Guthrie and Sitaraman to include that the network monitoring device responds to the unblock message by updating a network access list to authorize for Internet access the user whose network access device has the same hardware address as is embedded in the third identification code, as taught by Sitaraman, with the motivation of securing user domain access in a computer network (see Sitaraman, col. 1, lines 7-8).

In regards to claims 21-22, Levy teaches that the second identification code is further based on the Internet protocol address (i.e. IP address) of the network monitoring device. That is, Levy teaches that an IP address can be used to identify the source and destination in a communicating network. (see col. 8, lines 10-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to further modify the combination of Short, Levy, Guthrie and Sitaraman to include that the second identification code is further based on the Internet protocol address (i.e. IP address) of the network monitoring device with the motivation of using an effective way of identifying the source of a message in a communication network.

In regards to claim 23, Short teaches that the network monitoring device responds to the absence of the first predetermined identification code (i.e. authentication data) in a message whose destination is the authentication server by forwarding the message to said authentication server with no modification to the message (i.e. assuming that a user has not been authorized

access to the network based upon location based identification or user input identification, the user must provide the gateway device with sufficient information to become authorized access) (col. 13, lines 3-21).

In regards to claim 24, Short teaches that the network monitoring device is further effective for verifying if an out-going message is originated by an authorized user and permitting all out-going messages from authorized users unimpeded access to the Internet (i.e. after receiving the user's login information, the AAA server will create a user profile utilizing this information so that the user will be able to obtain immediate access to the network next time the user logs in without being required to enter login information again) (col. 13, lines 22-26),

all messages from unauthorized users having their destination addresses inspected to determine if their destination is said authentication server, and responding to a destination address other than said authentication server by ignoring the destination address and forwarding the message to a predetermined redirection server via the Internet (i.e. where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page) (col. 13, lines 7-9);

whereby all out-going messages to the Internet are granted access to the Internet irrespective of whether the message is originated by an unauthorized user (i.e.. SAT and HPR can intervene to direct the user to a webserver [external or internal] where the user has to login and identify themselves) (col. 12, lines 61-63).

In regards to claim 25, Short teaches that the redirection server responds to a received message from an unauthorized user by sending the user's network access device a message instructing it (i.e. redirecting it) to connect to the authentication server (i.e. where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page) (col. 13, lines 7-9).

14. Claims 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Levy in view of Guthrie in view of Sitaraman as applied to claim 19 above, in further view of Mishkin

In regards to claim 26 the combination of Short, Levy, Guthrie and Sitaraman teaches the system of claim 19 as discussed above.

Short also established that unauthorized messages are redirected to a login server and that identification keywords can be based on location (i.e. IP address) values.

The combination of Short, Levy, Guthrie and Sitaraman does not teach that the authentication server responds to a received message lacking the second identification code (i.e. not authorized) by generating a first predetermined identification code based on location information of said private network, and

that the authentication server further sends the network access device that originated the message a questionnaire form soliciting authentication information from its respective user, with the questionnaire form including a hidden reserved field and the first predetermined identification code.

Mishkin discloses a system for implementing and manipulating a session for a computer-based quiz (col.1, lines 10-11). The quiz of Mishkin is analogous to the questionnaire form of the instant invention. Mishkin teaches that the questionnaire form includes a hidden reserved field and a first identification keyword (i.e. at the top of the page are three fields: "instructor ID", "session name", and "student name". There is also a hidden field quizID pre-populated with "1234".) (col. 8, lines 1-3).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Short, Levy, Guthrie and Sitaraman with the teachings of Mishkin to include that the authentication server responds to a received message lacking the second identification code (i.e. not authorized) by generating a first predetermined identification code based on location information of said private network, and that the authentication server further sends the network access device that originated the message a questionnaire form soliciting authentication information from its respective user, with the questionnaire form including a hidden reserved field and the first predetermined identification code with the motivation to facilitate administration of the questionnaire forms (Mishkin, col. 1, lines 45-46).

In regards to claim 27, Mishkin teaches that said hidden reserved field is not accessible by the user that receives the questionnaire form. Mishkin teaches that the hidden field is pre-populated with "1234". This and the fact that the field is hidden suggest that the field cannot be accessed by said originator access device.

In regards to claim 30, Short teaches that the authentication server parses out the user's authentication information along with the hardware address from the second identification code; and that it relays that information to a gate keeper for verification (i.e. after receiving a request for access from a user, and identifying the user or location, the AAA server determines the access rights of the particular user.) (col. 12, lines 21-24). It can be inferred that the user or location are identified by extracting the contents of the hidden fields (i.e. account ID, hardware address, session ID, etc.).

Short does not teach that the gate keeper generates a third identification code and transmits it with an unblock message upon verification of the user.

Levy teaches that upon verification of the originator access device (i.e. access software application 411 in the portable computer 410) being registered, the gate keeper server decodes the contents of the hidden reserved field to determine the unique hardware address of the originator access device (i.e. MAC address) and that it labels the unblock message with said hardware address.

That is, Levy teaches that communication with the access software application is conducted by using a MAC address (col. 10, lines 21-36). Given that sending an unblock message is a way of communicating with the originator device, one can infer that a MAC address could be attached to the message, or that the message could be labeled with a MAC address. One would be motivated to label the unblock message with the MAC address of the originator device given the suggestion in Levy that this is a method of correctly representing the user (see Levy, col. 9, lines 65). Likewise, the unblock message could be labeled with any other identification keyword, including one generated by the gate keeper.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Levy, Guthrie and Sitaraman to include that the gate keeper generates a third identification code and transmits it with an unblock message upon verification of the user, as taught by Levy, with the motivation to correctly represent the user.

In regards to claim 31 Short teaches that the gate keeper is accessed via a secure link from the authentication server. In other words, the gate keeper of Short is contained with the authentication server (i.e. AAA server) therefore the link is secure.

In regards to claim 32, Short teaches that the authorization server accesses the gate keeper via the Internet (i.e. the login server can be an external/internal webserver) (col. 12, lines 61-63).

15. Claims 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Levy in view of Guthrie in view of Sitaraman in view of Mishkin as applied to claim 26 above, in further view of Lin.

In regards to claim 28, the combination of Short, Levy, Guthrie, Sitaraman and Mishkin teaches claim 26 as discussed above. It, however, does not teach that the hidden reserved field is preceded by the first predetermined identification code is the questionnaire form.

Lin teaches that when the server logic means returns a data packet, the channel ID and new state value are then hidden in the next HTML page that is sent to the web browser 211. In other words, each web page is used as a storage medium for maintaining channel ID and state

values for each ongoing session with a user of the web browser 211 (col. 10, lines 1-7). In other words, the Channel ID precedes the hidden reserved field (i.e. state value).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Levy, Guthrie, Sitaraman and Mishkin with the teachings of Lin to include that the hidden reserved field is immediately preceded by the first identification keyword within the out-going data packet with the motivation to maintain or utilize state information (see Lin, col. 9, lines 29-52).

16. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Short in view of Levy in view of Guthrie in view of Sitaraman in view of Mishkin as applied to claim 26 above, in further of Guthrie

In regards to claim 29, the combination of Short, Levy, Guthrie, Sitaraman and Mishkin teaches claim 26 as discussed above. It, however, does not teach that the monitoring device inserts the second identification code in the hidden field of any message sent by a user to the authentication server.

Guthrie teaches a personal authentication system. Guthrie teaches that an API reduces some of the processing overhead required for user authentication by the server 104. When the user is, for example, entering data to a form on a web page to request a certain process to be performed (e.g., by a common gateway interface (CGI) program), the user's account ID and previously generated response are attached to the form as a hidden field (col. 14, lines 28-48). In other words, Guthrie teaches the insertion of Ids into hidden fields for the purpose of user authentication.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Short, Levy, Guthrie, Sitaraman and Mishkin with the teachings of Guthrie to include that the monitoring device inserts the second identification code in the hidden field of any message sent by a user to the authentication server with the motivation to reduce the overhead required for user authentication.

Other Prior Art Made of Record

17. A. Lin et al. (U.S. Patent No. 6,282,575) discloses a routing mechanism for networks with separate upstream downstream traffic;

B. Van Horne et al. (U.S. Patent No. 6,460,084) discloses a forced network portal;

C. Guthrie et al. (U.S. Patent No. 6,161,185) discloses a personal authentication system and method for multiple computer platform; and

D. Grantges, Jr. et al. (U.S. Patent 6,510,464) discloses a secure gateway having routing feature.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H. Quiñones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheik can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quiñones
Patent Examiner
Technology Center 2100

February 25, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100